Scott Edward Cole, Esq. (S.B. #160744)
Teresa Denise Allen, Esq. (S.B. #264865)
Corey Benjamin Bennett, Esq. (S.B. #267816)
SCOTT COLE & ASSOCIATES, APC
1970 Broadway, Ninth Floor
Oakland, California 94612
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: scole@scalaw.com
Email: tallen@scalaw.com
Email: cbennett@scalaw.com
Web: www.scalaw.com

Timothy P. Rumberger, Esq. (S.B. #145984)
LAW OFFICES OF TIMOTHY P. RUMBERGER
1339 Bay Street
Alameda, California 94501
Telephone: (510) 841-5500
Facsimile: (510) 521-9700
Email: tim@rumbergerLaw.com

Attorneys for Representative Plaintiff
and the Plaintiff Class(es)

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

ANDREW GALPERN, individually, and on behalf of all others similarly situated, Plaintiffs, vs. EQUIFAX, INC., TRUSTED ID, INC. Defendants.	**Case No.** **CLASS ACTION** **COMPLAINT FOR DAMAGES, RESTITUTION, INJUNCTIVE/EQUITABLE RELIEF** ***JURY TRIAL DEMANDED***

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

Representative Plaintiff alleges as follows:

INTRODUCTION

1. This is a class action brought by Representative Plaintiff on behalf of himself as well as on behalf of California and national classes of all entities/persons whose personally identifiable information was acquired by unauthorized persons in the Data Breach announced by Equifax, Inc. ("Equifax") in September 2017.

2. Specifically, on September 7, 2017, Equifax Inc. announced that, starting as early as May 2017, hackers had breached a Web-based application for Equifax and obtained sensitive personal information of approximately 143 million American consumers. The personal information obtained in the breach included social security numbers, birth dates and home addresses. Equifax also said it lost control of an unspecified number of driver's license numbers, along with the credit card numbers of 209,000 consumers and credit dispute documents for 182,000 consumers. While Equifax admits it learned of the breach as early as July 2017, it elected to keep this information secret from the public until September 2017. These events are hereinafter referred to as the "Data Breach."

3. As a result of these events, Representative Plaintiff, on behalf of himself and members of each of the respective classes (hereinafter "class members" in one or more of the classes identified herein), seeks damages, interest thereon, restitution, injunctive and other equitable relief, reasonable attorneys' fees and costs as a result of Equifax's numerous unlawful and/or deceptive business practices, as detailed herein.

4. As detailed further herein, Representative Plaintiff asserts that Equifax engaged in reckless conduct by, *inter alia*, failing to secure and safeguard consumers' personally identifiable information ("Personal Information") which Equifax collected from various sources in connection with its operation as a consumer credit reporting agency, and for failing to provide timely, accurate and adequate notice to class members that their Personal Information had been wrongfully obtained, and precisely what types of information were wrongfully obtained.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

JURISDICTION AND VENUE

5. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction) and/or 28 U.S.C. §1331 (controversy arising under United States law). Supplemental jurisdiction to adjudicate issues pertaining to California state law is proper in this Court under 28 U.S.C. §1367.

6. Equifax routinely conducts business in California, has sufficient minimum contacts in California and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within California.

7. Venue is proper in this Court under 28 U.S.C. § 1391 and Local Rule 3-2.c., because the events that gave rise to Representative Plaintiff's claims took place within the Northern District of California, and Equifax does business in this Judicial District. Moreover, assignment to the San Jose Division is proper because a substantial part of the events and omissions which gave rise to the claims occurred at TrustedID's headquarters in Palo Alto, California

REPRESENTATIVE PLAINTIFF

8. Plaintiff Andrew Galpern is adult individual and resident of the State of California. He is referred to in this Complaint as the "Representative Plaintiff" and/or simply as "Plaintiff." Plaintiff is a victim of the Data Breach.

9. At all times herein relevant, Representative Plaintiff is and was a member of the National class and the California Subclass.

10. Representative Plaintiff brings this action on behalf of himself, and as a class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of all persons similarly situated and proximately damaged by the unlawful conduct described herein.

//

//

//

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

DEFENDANTS

11. Defendant Equifax, Inc. is a Delaware corporation with its principal place of business located at 1550 Peachtree Street NE, Atlanta, Georgia 30309.

12. Equifax, Inc. is a global information services provider, one of the three largest credit reporting agencies in the United States, a credit monitoring company, and a data broker. It "organizes, assimilates and analyzes data on more than 820 million consumers and roughly 90 million businesses worldwide."

13. In turn, Equifax provides credit information services to millions of businesses, governmental units, and consumers across the globe. Equifax operates through various subsidiaries including Equifax Information Services, LLC, and Equifax Consumer Services, LLC (aka Equifax Personal Solutions, or PSOL). Each of these entities acted as agents of Equifax or, in the alternative, acted in concert with Equifax as alleged in this Complaint.

14. Defendant TrustedID Inc. is incorporated in Delaware and headquartered in Palo Alto, California.

CLASS ACTION ALLEGATIONS

15. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of himself and the following classes/subclass(es) (collectively, the "classes"):

> California class:
> "All consumers within the State of California whose personal or credit data was stored by Equifax and/or was accessed by hackers in the Data Breach announced by Equifax in September 2017."
>
> National class:
> "All consumers within the United States of America whose personal or credit data was stored by Equifax and/or was accessed by hackers in the Data Breach announced by Equifax in September 2017."

16. Defendants, and their officers, directors and employees, as well as the Judge assigned to this matter, and all staffers of Plaintiff's counsel's law firms are excluded from each

of the Plaintiff classes.

17. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed classes is easily ascertainable:

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiff is informed and believes and, on that basis, alleges that the total number of class members is in the millions of individuals. Membership in the classes will be determined by analysis of Equifax's records.

b. Commonality: The Representative Plaintiff and the class members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Equifax had a legal duty to Plaintiff and the classes to exercise due care in collecting, storing, and safeguarding their Personal Information;

2) Whether Equifax knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Equifax's security measures to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Equifax was negligent in failing to implement reasonable and adequate security procedures and practices;

5) Whether Equifax's failure to implement adequate data security measures allowed the Data Breach to occur;

6) Whether Equifax failed to timely notify the public of the Data Breach;

7) Whether Equifax's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Personal Information of Plaintiff and class members;

8) Whether Equifax's conduct constituted deceptive trade practices; and

9) Whether injunctive, corrective and/or declaratory relief and/or an accounting is appropriate.

c. Typicality: The Representative Plaintiff's claims are typical of the claims of the Plaintiff classes. Representative Plaintiff and all members of the Plaintiff classes sustained damages arising out of and caused by

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

Defendants' common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: The Representative Plaintiff in this class action is an adequate representative of each of the Plaintiff classes in that the Representative Plaintiff has the same interest in the litigation of this case as the class members, is committed to vigorous prosecution of this case and has retained competent counsel who is experienced in conducting litigation of this nature. The Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other class members or the classes in their entirety. The Representative Plaintiff anticipates no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual class members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Plaintiff classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other class members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

COMMON FACTUAL ALLEGATIONS

Defendants' Unlawful Conduct

18. On September 7, 2017, Equifax announced that hackers had illicitly accessed its computer systems that warehoused data on approximately half of the U.S. population. The hackers used a "U.S. website application vulnerability" to gain access to Equifax's systems, and allegedly remained undetected for approximately two-and-a-half months. During that time, they compromised the personal information of approximately 143 million Americans.

19. Thus far, Equifax has admitted that credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed.

20. The compromised data includes names, birth dates, and Social Security numbers. Equifax also allowed the hackers to steal driver's license numbers, credit card information, and other credit history details about hundreds of thousands of consumers. Equifax's statements following the breach indicate that it failed to adopt reasonable security measures relating to

perimeter security, application patching, and network segmentation, adequate to ensure that consumers' information was safe inside its computer network.

21. This was not the first time that hackers have exploited Equifax's sub-par cybersecurity controls. Equifax data has been taken during at least four previous data breaches. In March 2014, Equifax reported a breach that occurred between April 2013 and January 2014, in which customer credit reports were compromised. In May 2016, Equifax's W-2 Express website suffered a breach that resulted in the compromise of 430,000 names, addresses, Social Security numbers and other personal information. In February 2017, Equifax "was forced to confess to a data leak in which credit information of a 'small number' of customers at partner LifeLock had been exposed to another user of the latter's online portal." Finally, and most recent before the instant breach, in May 2017, TALX, an Equifax subsidiary that provides online payroll and HR services, suffered a breach in which hackers were able to obtain customer W-2 tax data.

22. As a result of the sensitive nature of the information it harvested and held, not to mention these prior breaches, Equifax was well aware it presented an attractive target for hackers, yet failed to take industry standard steps to protect the data.

23. With regard to the instant breach, Equifax knew about it for several weeks before announcing it. Indeed, the company acknowledged that it discovered the unauthorized access on July 29 2017, but has failed to inform the public why it delayed notification of the Data Breach to consumers. Instead, Equifax executives sold at least $1.8 million worth of shares before the public disclosure of the breach. It has been reported that its Chief Financial Officer John Gamble sold shares worth $946,374, its President of U.S. Information Solutions, Joseph Loughran, exercised options to dispose of stock worth $584,099, and its President of Workforce Solutions, Rodolfo Ploder, sold $250,458 of stock on August 2, 2017.

24. When Equifax finally disclosed the incident, it directed consumers to visit a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been "potentially impacted" by the breach and to enable them "to sign up for credit file monitoring and identity theft protection."

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

25. Equifax's dedicated website said that, if consumers entered their last name and the last six digits of their Social Security number, the website would tell them whether their information had been taken in the breach.

26. The Equifaxsecurity2017.com site also tells consumers that Equifax is offering one free year of TrustedID Premier credit monitoring services, which includes "five separate offerings," including: free copies of your Equifax credit report, bureau credit file monitoring, the ability to lock your Equifax credit file, $1 million of identity theft insurance, and Social Security Number Monitoring—a service that searches the dark web for criminals attempting to sell your Social Security number.

27. This website further explains that, in addition to people impacted by the Data Breach, Equifax is offering one year of free TrustedID Premier services to anyone in the United States, "[r]egardless of whether your information may have been impacted."

28. However, what Equifax does not disclose (in its press release or on its breach website) is that Equifax bought TrustedID Inc. in 2013. The TrustedID Premier product is an identity monitoring service owned and operated by Equifax.

29. Equifax could have offered identity monitoring services through its own branded service, "Equifax ID Patrol," but chose to instead offer credit monitoring services through its subsidiary, TrustedID.

30. Thus, by encouraging all consumers to sign up for TrustedID Premier, Equifax stands to profit significantly from the breach of its own computer network. Equifax intends to exploit its own exposure to hacking in precisely this manner.

31. Such conduct shouldn't be a surprise. Indeed, in its 2016 10-K filing with the Securities and Exchange Commission, Equifax noted that many credit monitoring companies were increasingly pursuing a business strategy of "offering free or low-cost direct to consumer credit services (such as credit scores, reports, and monitoring)" and using those free "services as a means to introduce consumers to premium products and services."

32. In a 2014 presentation to investors, Equifax said that one of its "key growth strategies" was to "attack" the $1.6 billion market for non-financial institution products, such as

credit monitoring, by utilizing its acquisition of TrustedID as a "foundation." There, Equifax explained that "the US identity protection market [is] estimated to be a US$1.6 billion industry."

33. Much of Equifax's revenue growth has come from its sale of identity protection through TrustedID. Equifax noted in its Annual Statement to investors that it had boosted revenue by 12% in 2013 due to increased sales of "U.S.-based subscription services," sales that were spurred by "the acquisition of TrustedID" in 2013.

34. Equifax's 10-K disclosures show that it earned $402.6 million in revenue from its "Global Consumer Solutions" division in 2016. Equifax explains that "Global Consumer Solutions revenue" is "derived from the sale of credit monitoring and identity theft protection products, which [Equifax] delivers to consumers primarily via the internet."

35. By these acts, Equifax is attempting to capitalize on the breach of its computer systems by using it as an opportunity to try to carve out a larger share of the $1.6 billion identity protection industry.

36. Equifax also benefits when consumers sign up for TrustedID services by gaining access to a wider trove of data. TrustedID's service monitors all three credit bureaus. To sign up, a consumer must authorize TrustedID to retrieve his information from the other two credit bureaus (Experian and TransUnion). The information on the credit reports of the bureaus can vary by up to 20%, meaning Equifax can gain access to additional information from the other two credit bureaus when consumers grant TrustedID access to their Experian and TransUnion credit files.

37. In addition, Equifax's fraud alert product for its three-bureau monitoring is "made available to consumers by Equifax Information Services LLC." Equifax Information Services LLC is a data broker that sells consumer information. In 2012, Equifax Information Services LLC settled a lawsuit brought by the Federal Trade Commission over its allegedly unlawful selling of consumers' information to third parties who pitched predatory debt relief services to consumers in financial distress.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

38. When consumers sign up for TrustedID, they are purportedly agreeing to allow TrustedID to share their personal information with TrustedID's "affiliates"—which include Equifax Information Services LLC.

Defendants' Breaches and Harm to Consumers

39. Personal data such as that hacked in the Data Breach represents a major score for cybercriminals who will likely look to capitalize on it by launching targeted phishing campaigns.

40. Indeed, it is well known and the subject of many media reports that Personal Information is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, Equifax maintained an insufficient and inadequate system to protect the Personal Information of Plaintiff and class members.

41. Personal Information is a valuable commodity for which a "cyber blackmarket" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. Personal Information is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

42. Legitimate organizations and the criminal underground alike recognize the value in Personal Information contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing Personal Information] from 38 million users." (See, Verizon 2014 PCI Compliance Report, available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci201 4.pdf , at 54).

43. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." (See, 17 C.F.R. §248.201). The FTC further describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

44. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance." See, Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 10, 2017).

45. Identity thieves can use personal information, such as that of Plaintiff and class members which Equifax failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

46. At all relevant times, Equifax was well-aware, or reasonably should have been aware, that the Personal Information collected, maintained and stored in the POS systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

47. As a result of the Equifax Data Breach, the Personal Information of the Plaintiff and class members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and class members, or likely to be suffered by Plaintiff and class members as a direct result of the Equifax Data Breach include:

a. unauthorized use of their Personal Information;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their Personal Information;

e. loss of privacy;

f. loss of use of and access to their account funds and costs associated with

inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

g. unauthorized charges on their debit and credit card accounts;

h. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

i. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals and already misused via the sale of Plaintiff's and class members' information on the Internet black market;

j. damages to and diminution in value of their Personal Information entrusted to Equifax for the sole purpose of purchasing products and services from Equifax; and the loss of Plaintiff's and class members' privacy;

48. The injuries to the Plaintiff and the class members were directly and proximately cause by Equifax's failure to implement or maintain adequate data security measures for Personal Information.

49. The Data Breach was the inevitable result of Equifax's inadequate approach to data security and the protection of the Personal Information that it collected during the course of its business and, as such, Equifax could have prevented this Data Breach. It had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

50. Had Equifax remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Equifax would have prevented the Data Breach and, ultimately, the theft of its customers' Personal Information.

//

//

//

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

FIRST CLAIM FOR RELIEF
NEGLIGENCE
(for the California and National Classes versus Equifax)

51. Representative Plaintiff incorporates in this cause of action every allegation of the preceding paragraphs, with the same force and effect as though fully set forth herein.

52. At all times herein relevant, Equifax owed Representative Plaintiff and members of both classes a duty of care, *inter alia*, to act with reasonable care to secure and safeguard the Personal Information of Plaintiff and class members and to use commercially reasonable methods to do so. Equifax took on this obligation upon accepting and storing the Personal Information of Plaintiff and class members in its computer systems and on its networks.

53. Among these duties, Equifax was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Personal Information in its possession;

b. to protect Personal Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches.

54. Equifax knew that the Personal Information was private and confidential and should be protected as private and confidential and, thus, Equifax owed a duty of care not to subject Plaintiff, along with his Personal Information, and class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

55. Equifax knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches.

56. Equifax knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and class members' Personal Information. Equifax breached its duties to Plaintiff and class members by failing to provide fair, reasonable, or adequate computer

systems and data security practices to safeguard Personal Information of Plaintiff and class members.

57. Because Equifax knew that a breach of its systems would damage millions of individuals, including Plaintiff and class members, Equifax had a duty to adequately protect its data systems and the Personal Information contained thereon.

58. Plaintiff's and class members' willingness to entrust Equifax with their Personal Information was predicated on the understanding that Equifax would take adequate security precautions. Moreover, only Equifax had the ability to protect its systems and the Personal Information it stored on them from attack.

59. Equifax had a special relationship with Plaintiff and class members.

60. Equifax also had independent duties under state and federal laws that required Equifax to reasonably safeguard Plaintiff's and class members' Personal Information and promptly notify them about the Data Breach.

61. Equifax did breach its general duty of care to Representative Plaintiff and members of both classes in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Personal Information of Plaintiff and class members;

b. by failing to timely and accurately disclose that Plaintiff's and class members' Personal Information had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard Personal Information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Personal Information;

d. by failing to provide adequate supervision and oversight of the Personal Information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Personal Information of Plaintiff and class members, misuse the Personal Information and intentionally disclose it to others without consent.

62. The law further imposes an affirmative duty on Equifax to timely disclose the unauthorized access and theft of the Personal Information to Plaintiff and the classes so that

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

Plaintiff and class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information.

63. Equifax breached its duty to notify Plaintiff and class members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiff and class members and then by failing to provide Plaintiff and class members information regarding the breach until September 2017. Instead, its executives disposed of at least $1.8 million worth of shares in the company after Equifax learned of the Data Breach but before it was publicly announced. To date, Equifax has not provided sufficient information to Plaintiff and class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the classes.

64. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Equifax prevented Plaintiff and class members from taking meaningful, proactive steps to secure their financial data and bank accounts.

65. As a direct and proximate result of Equifax's actions, Representative Plaintiff and members of both classes have suffered and continue to suffer economic losses and other general and specific damages, including, but not limited to damages (1) arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Personal Information, (2) arising from Plaintiff's inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards, and (3) from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing freezes and alerts with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, all in an amount to be proven at trial.

//

//

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

SECOND CLAIM FOR RELIEF
NEGLIGENCE PER SE
(for the California and National Classes versus Equifax)

66. Representative Plaintiff incorporates in this cause of action every allegation of the preceding paragraphs, with the same force and effect as though fully set forth herein.

67. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described above also form part of the basis of Equifax's duty in this regard.

68. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiff and class members.

69. Equifax's violation of Section 5 of the FTC Act constitutes negligence *per se*.

70. Plaintiff and class members are within the class of persons that the FTC Act was intended to protect.

71. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the classes.

72. As a direct and proximate result of Equifax's actions, Representative Plaintiff and members of both classes have suffered and continue to suffer economic losses and other general and specific damages, including, but not limited to damages (1) arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use

of the Personal Information, (2) arising from Plaintiff's and class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards, and (3) from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing freezes and alerts with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, all in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT (FCRA)
(for the California and National Classes versus Equifax)

73. Representative Plaintiff incorporates in this cause of action every allegation of the preceding paragraphs, with the same force and effect as though fully set forth herein.

74. As individuals, Plaintiff and class members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

75. Under the FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

76. Equifax is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

77. As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

78. Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1).

79. The compromised data was a consumer report under the FCRA because it was a communication of information bearing on class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the class members' eligibility for credit.

80. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a).

81. None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the National class members' Personal Information.

82. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

83. Equifax furnished the National class members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

84. The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the FCRA, in connection with data breaches.

85. Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under §1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

86. Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiff and other members of the classes of their rights under the FCRA.

87. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiff's and National class members' personal information for no permissible purposes under the FCRA.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

88. Plaintiff and the National class members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiff and each of the National class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

89. Plaintiff and the National class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) & (3).

FOURTH CLAIM FOR RELIEF
UNFAIR BUSINESS
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT (FCRA)
(for the California and National Classes versus Equifax)

90. Representative Plaintiff incorporates in this cause of action every allegation of the preceding paragraphs, with the same force and effect as though fully set forth herein.

91. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under § 1681b of the FCRA.

92. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

93. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiff's and the class members' Personal Information and consumer reports for no permissible purposes under the FCRA.

94. Plaintiff and the class members have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiff and each of the class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

95. Plaintiff and the class members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

FIFTH CLAIM FOR RELIEF
CALIFORNIA CUSTOMER RECORDS ACT: CAL. CIV. CODE, §1798.80, *ET SEQ.*
(for the California Class Only versus Equifax)

96. Representative Plaintiff incorporates in this cause of action every allegation of the preceding paragraphs, with the same force and effect as though fully set forth herein.

97. Plaintiff brings this cause of action on behalf of the California class whose personal information is maintained by Equifax and/or that was compromised in the Data Breach announced in September 2017.

98. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted California Customer Records Act. This statute states that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Civil Code § 1798.81.5.

99. Equifax is a "business" within the meaning of Civil Code § 1798.80(a).

100. Plaintiff and members of the California class are "individual[s]" within the meaning of the Civil Code § 1798.80(d). Pursuant to Civil Code §§ 1798.80(e) and 1798.81.5(d)(1)(C), "personal information" includes an individual's name, Social Security number, driver's license or state identification card number, and debit card and credit card information. "Personal information" under Civil Code §1798.80(e) also includes address, telephone number, passport number, education, employment, or employment history.

101. The breach of the personal data of over one hundred million Equifax consumers instituted a "breach of the security system" of Equifax pursuant to Civil Code §1798.82(g).

102. By failing to implement reasonable measures to protect its consumers' personal data, Equifax violated Civil Code §1798.81.5.

103. In addition, by failing to promptly notify all affected consumers that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the Data Breach, Equifax violated Civil Code § 1798.82 of the same title. Equifax's failure to timely notify consumers of the breach has caused damage to class

members who have had to buy identity protection services or take other measures to remediate the breach caused by Equifax's negligence.

104. By violating Civil Code §§1798.81.5 and 1798.82, Equifax "may be enjoined" under Civil Code §1798.84(e).

105. Accordingly, Plaintiff requests that the Court enter an injunction requiring Equifax to implement and maintain reasonable security procedures to protect customers' data in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that Equifax, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis; (2) ordering that Equifax engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Equifax, consistent with industry standard practices, conduct regular database scanning and securing checks; (5) ordering that Equifax, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (7) ordering Equifax to encrypt sensitive personal information.

106. Plaintiff further requests that the Court require Equifax to (1) identify and notify all members of the class who have not yet been informed of the Data Breach; and (2) to notify affected former and current consumers of any future data breaches by email within 24 hours of Equifax's discovery of a breach or possible breach and by mail within 72 hours.

107. As a result of Equifax's violation of Civil Code §§ 1798.81.5, and 1798.82, Plaintiff and members of the class have and will incur economic damages relating to time and money spent remedying the breach, including but not limited to, expenses for bank fees associated with the breach, any unauthorized charges made on financial accounts, lack of access to funds while banks issue new cards, tax fraud, as well as the costs of credit monitoring and purchasing credit reports.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

108. Plaintiff, individually and on behalf of the members of the California class, seeks all remedies available under Civil Code §1798.84, including, but not limited to: (a) damages suffered by members of the class; and (b) equitable relief.

SIXTH CLAIM FOR RELIEF
UNFAIR BUSINESS PRACTICES UNDER THE UNFAIR COMPETITION ACT: CAL. BUS. & PROF. CODE, §17200, *ET SEQ.*

(for the California Class Only versus All Defendants)

109. Representative Plaintiff incorporates in this cause of action every allegation of the preceding paragraphs, with the same force and effect as though fully set forth herein.

110. Representative Plaintiff and members of the California class further bring this cause of action, seeking equitable and statutory relief to stop the misconduct of Equifax, as complained of herein.

111. The knowing conduct of Equifax, as alleged herein, constitutes an unlawful and/or fraudulent business practice, as set forth in California Business & Professions Code §§17200-17208. Specifically, Equifax conducted business activities while failing to comply with the legal mandates cited herein, including the FCRA. Such violations include but are not necessarily limited to:

a. failure to maintain adequate computer systems and data security practices to safeguard Personal Information;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard Personal Information from theft;

c. failure to timely and accurately disclose the Data Breach to Plaintiff and class members;

d. continued acceptance of Personal Information and storage of other personal information after Equifax knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. continued acceptance of Personal Information and storage of other personal information after Equifax knew or should have known of the Data Breach and before it allegedly remediated the Breach;

112. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the Personal Information of Plaintiff and California class

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

113. In engaging in these unlawful business practices, Equifax has enjoyed an advantage over its competition and a resultant disadvantage to the public and California class members.

114. Equifax's knowing failure to adopt policies in accordance with and/or adhere to these laws, all of which are binding upon and burdensome to Equifax's competitors, engenders an unfair competitive advantage for Equifax, thereby constituting an unfair business practice, as set forth in California Business & Professions Code §§17200-17208.

115. Equifax has clearly established a policy of accepting a certain amount of collateral damage, as represented by the damages to Representative Plaintiff and members of the California class herein alleged, as incidental to its business operations, rather than accept the alternative costs of full compliance with fair, lawful and honest business practices ordinarily borne by responsible competitors of Equifax and as set forth in legislation and the judicial record.

116. Representative Plaintiff and members of the California class request that this Court enter such orders or judgments as may be necessary to enjoin Equifax from continuing its unfair, unlawful, and/or deceptive practices and to restore to Representative Plaintiff and members of the California class any money Equifax acquired by unfair competition, including restitution and/or restitutionary disgorgement, as provided in Cal. Bus. & Prof. Code §17200, *et seq.*; and for such other relief set forth below.

REQUEST FOR RELIEF

WHEREFORE, the Representative Plaintiff, on behalf of himself and each member of the proposed National Class and the California Subclass, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendants, and each of them, jointly and separately, as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiff's counsel as Class Counsel;

2. For an award to Representative Plaintiff and members of both classes of compensatory and special damages in an amount to be proven at trial;

3. That Defendants be found to have made negligent misrepresentations/omissions of fact to Representative Plaintiff and members of both classes;

4. That the Court enjoin Defendants, ordering them to cease and desist from unlawful activities in further violation of California Business and Professions Code §17200, *et seq.*;

5. For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and class members' Personal Information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and class members;

6. For equitable relief compelling Equifax to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to class members the type of Personal Information compromised;

7. Access to a free credit report twice a year be made available to every consumer whose Personal Information was obtained in the security breach, pursuant to 15 USC §1681c-1, (a)(2)(A);

8. A "Fraud Alert" placed on the file of every consumer whose Personal Information was obtained in the security breach, pursuant to 15 USC §1681c-1, (a)(1)(A-B), and communicated to the other Credit Reporting Agencies;

9. For interest on the amount of any and all economic losses, at the prevailing legal rate;

10. For an award of punitive and/or exemplary damages, in an amount sufficient to deter such conduct in the future;

11. For an award of reasonable attorneys' fees, pursuant to California Code of Civil Procedure §1021.5, *inter alia*;

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800

12. For costs of suit and any and all other such relief as the Court deems just and proper;

13. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiff and members of each of the Plaintiff classes hereby demand trial by jury on all issues triable of right by jury.

Dated: September 12, 2017

SCOTT COLE & ASSOCIATES, APC

By: /s/ Scott Edward Cole
Scott Edward Cole, Esq.
Attorneys for Representative Plaintiff
and the Plaintiff class(es)

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
THE TOWER BUILDING
1970 BROADWAY, NINTH FLOOR
OAKLAND, CA 94612
TEL: (510) 891-9800